Parfilova Maria Alexandrovna
Student
Ural Federal University named after the first
President of Russia B.N. Yeltsin
Russia, Ekaterinburg
Academic supervisor: Kovaleva Alexandra Georgievna

CYBER RISK AND INSURANCE FOR TRANSPORTATION INFRASTRUCTURE

Abstract. *The article is devoted to the topic of cyber risk and insurance in the scope of transportation infrastructure. The aim of the article is to identify the barriers to a robust cyber insurance market and improved cyber resilience for transportation infrastructure. This is accomplished through a mixed methods approach involving analysis of cyber incident data for transportation systems and a series of interviews with transportation infrastructure managers and insurers. The approach allows making a comparison of subjective versus objective cyber risk.*

Keywords: *cyber risk, insurance, transportation infrastructure, incident frequency, cybersecurity, infrastructure manager, insurer.*

Парфилова Мария Александровна
Студент
Уральский федеральный университет имени Первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
Научный руководитель: Ковалёва Александра Георгиевна

КИБЕРРИСК И СТРАХОВАНИЕ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ

Аннотация: *Статья посвящена теме киберриска и страхования в сфере транспортной инфраструктуры. Цель этой статьи - анализ путей достижения устойчивого рынка киберстрахования и усовершенствования кибербезопасности транспортной инфраструктуры. Это достигается при помощи смешанного подхода, включающего в себя анализ данных киберинцидентов и серии интервью с менеджерами транспортной инфраструктуры и страховщиками. Данный подход позволит сравнить субъективный и объективный киберриски.*

Ключевые слова: *киберриск, страхование, транспортная инфраструктура, частота инцидентов, кибербезопасность, менеджеры инфраструктуры, страховщик.*

Cyber risk and insurance in the scope of transportation infrastructure are explored in this article. The chosen methods and data for analyzing trends in cyber vulnerability of transport infrastructure are considered. The transport cyber incident data and interviews with transport infrastructure managers and insurers to characterize current cyber risk perceptions are discussed. The approach is used to study the history of cyber incidents. The study includes companies only in the field of transport infrastructure.

There are three aspects of the dataset for understanding the evolution of transportation cyber incidents:

1) the number of companies affected from 2006 to 2014,
2) the amount of losses,
3) types of incidents.

The sample contains 284 incidents. The numbers show the trend in cyber risks in the transportation infrastructure industry. Transport companies must disclose related cyber incidents after 2006 according legal requirement. That is why, the number of cyber incidents and affected firms increased since 2006 reflects a real increase in cyber risks [4].

The ratio of Incidents/Companies roughly stays at the same level over time, except for 2006 (Figure 1). In addition, until 2009, the number of incidents and the number of company events affected in the transport infrastructure industry declined annually. However, from 2009 to 2014, both numbers are growing 0.

The number of affected companies usually moves in the same direction as the total number of companies, except for 2010. In 2010, the total number decreased comparing to the previous year, but the number of affected companies increased.

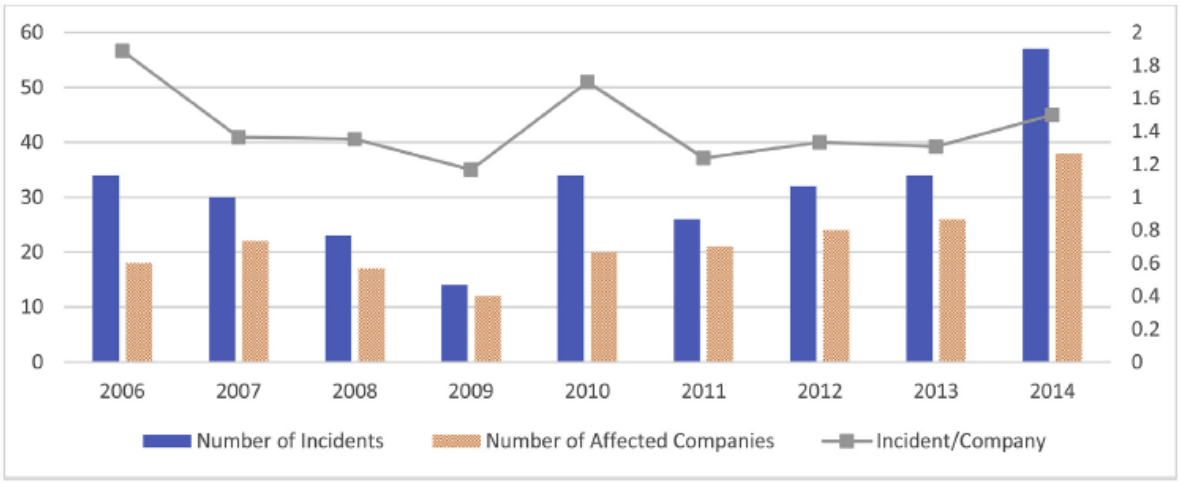

Figure 1 – Cyber incident number and affected company number over time 0.

These results indicate that cyber risk is affecting the growing share of companies in the transportation infrastructure industry over time, and that the increase in affected companies is indeed driven by the spread of cyber risk. This suggests that companies in the industry may experience cyber incidents.

The yearly average loss resulting from one cyber incident is commonly below $10 million and slowly increasing in the next years (Figure 2). The maximum losses of 2013 and 2014 years caused by a single incident increases with much faster speed. This signifies that the losses of victim companies are becoming more unbearable. If this trend continues, companies will have to consider transferring some part of the risk and one way is applying to cyber insurance. This points to an increase in demand for cyber insurance in the transportation infrastructure industry 0.

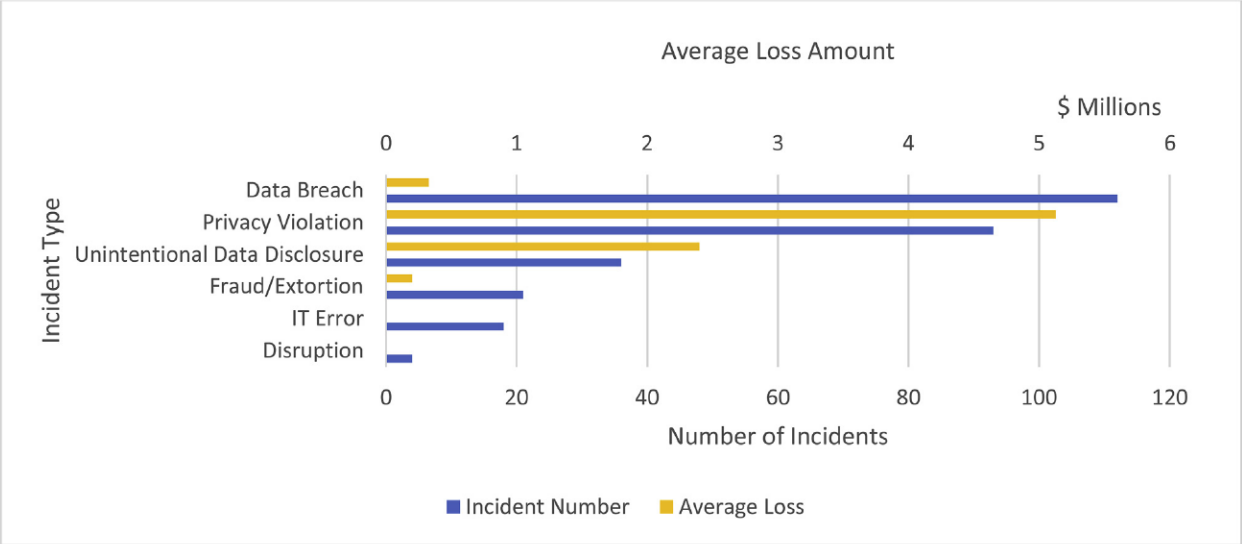

Figure 2 – Frequency and severity by incident type. 0

Cyber risk canmay lead to a variety of incident kinds. In the transportation infrastructure industry, the most overall one is a data breach, which is a leak of confidential information caused by intruders or the loss of storage devices. Data violations account for 39.4% (112) of all incidents, and they result in an average loss of $ 0.33 million per incident according to figure 2.

Privacy-related incidents also have a very high occurrence frequency. These incidents include contacting, collecting data from, and spreading information without permission, and they are 32.7% (93) of the incidents with the average loss of $5.13 million per incident. That is the highest indicator among all incidents [2].

Unintentional data disclosure also has loss at $3.17 million per incident. These kind of incidents are usually a consequence of company's not complying the information disclosure terms. Both privacy violations and unintentional data disclosures take place at the cyber-system layers, which allow the system interaction with the environment. These risks may be softened by realization of privacy protection and advancement of security education. 0

Cyber fraud and extortion are incidents wherein attackers deceive victims into transferring money. For example, phishing scams, or compulsion them into paying ransom to recover violated data or systems. Therefore, beyond improving

cybersecurity, backup plans are vital to reducing business interruption costs in these types of incidents.

IT errors happen when companies make configuration changes to infrastructure or implement new systems. The analysis of the data demonstrates that the incident frequency and the potential loss severity of cyber incidents are growing in the scope of transportation infrastructure. The possibility of companies to be hit by at least one cyber incident is growing annually, and the sum of losses is constantly increasing.

The current state of cyber insurance for transportation infrastructure based on the received information from informal interviews with insurers and infrastructure managers is important. Infrastructure managers are concerned about cyber risks and partly understand their influence on the situation. In addition, they currently have a lack of tools to assess and deal with cyber risks. Some infrastructure managers procured cyber insurance for cyber protection but find the existing cyber insurance products to be not satisfying exactly their needs [3]. Insurers point out that there are dependencies on policy limits connected with unknown risk character. Since a cyber risk is not enough studied, infrastructure managers want cyber policies with a broad range of coverage.0

In accordance with all the above, there are four main lines of research that are needed to improve the management and insurance of cyber risks for transport infrastructure systems:

1) data and models of cyber incidents,
2) cyber risk metrics,
3) understanding the perceived possibility and impact of cyberattacks,
4) new and more reliable cyber insurance products.

Finally, each solution provides only some level of security. Even after the development of improved tools and making models the residual cyber risk is crucial, and buying insurance is an essential management strategy to enable transportation infrastructure systems to recover from cyber events. Further research of the type and management of cyber risks is needed to support policies and management strategies to address this growing risk of transport systems.

REFERENCES

1. Cyber risk and insurance for transportation infrastructure. – 2019. – [Text: electronic]. – URL: https://www.sciencedirect.com/science/article/abs/pii/S0967070X18307248 (Reference date 10.10.2020).

2. ARIES: Evaluation of a reliable and privacy-preserving European identity management framework. –2020. – [Text: electronic]. – URL: https://www.sciencedirect.com/science/article/abs/pii/S0167739X1930843X (Reference date 25.09.2020).

3. Data science and analytics in aviation. – 2020. – [Text: electronic]. – URL: https://www.sciencedirect.com/science/article/abs/pii/S1366554520300077 (Reference date 07.11.2020).

4. Aviation cybersecurity and cyber-resilience: assessing risk in Air Traffic Management. – 2019. – [Text: electronic]. – URL: https://www.researchgate.net/publication/330071672_Aviation_Cybersecurity_and_Cyber-Resilience_Assessing_Risk_in_Air_Traffic_Management_Theories_Methods_Tools_and_Technologies (Reference date 11.10.2020).